



UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office

Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
09/493,031	01/28/00	SAMID	G 4427-002

TM02/0112
BLANK ROME COMISKY & MCCAULEY, LLP
THE FARRAGUT BUILDING, SUITE 1000
930 17TH STREET, N.W.
WASHINGTON DC 20006

EXAMINER

SEAL, J

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED:

01/12/01

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

Office Action Summary

Application No.
09/493,031

Applicant(s)

Samid

Examiner

James Seal

Group Art Unit

2766

☒ Responsive to communication(s) filed on 1 Nov 2000

☒ This action is **FINAL**.

☐ Since this application is in condition for allowance except for formal matters, **prosecution as to the merits is closed** in accordance with the practice under *Ex parte Quayle*, 35 C.D. 11; 453 O.G. 213.

A shortened statutory period for response to this action is set to expire 3 month(s), or thirty days, whichever is longer, from the mailing date of this communication. Failure to respond within the period for response will cause the application to become abandoned. (35 U.S.C. § 133). Extensions of time may be obtained under the provisions of 37 CFR 1.136(a).

Disposition of Claim

☒ Claim(s) 1-33 is/are pending in the application.

Of the above, claim(s) 6, 14, and 15 is/are withdrawn from consideration.

☐ Claim(s) _____ is/are allowed.

☒ Claim(s) 1-5, 7-13, and 16-33 is/are rejected.

☐ Claim(s) _____ is/are objected to.

☐ Claims _____ are subject to restriction or election requirement.

Application Papers

☐ See the attached Notice of Draftsperson's Patent Drawing Review, PTO-948.

☒ The drawing(s) filed on 1 Nov 2000 is/are objected to by the Examiner.

☐ The proposed drawing correction, filed on _____ is ☐ approved ☐ disapproved.

☐ The specification is objected to by the Examiner.

☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

☐ Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

☐ All ☐ Some* ☒ None of the CERTIFIED copies of the priority documents have been

☐ received.

☐ received in Application No. (Series Code/Serial Number) _____.

☐ received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

*Certified copies not received: _____

☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

Attachment(s)

☒ Notice of References Cited, PTO-892

☐ Information Disclosure Statement(s), PTO-1449, Paper No(s). _____

☐ Interview Summary, PTO-413

☐ Notice of Draftsperson's Patent Drawing Review, PTO-948

☐ Notice of Informal Patent Application, PTO-152

--- SEE OFFICE ACTION ON THE FOLLOWING PAGES ---

Art Unit: 2766

DETAILED ACTION

1. This action is a response to your correspondence of 1 November 2000.
2. Amended claims 1, 7, 9, 10, and 16 have been entered and approved.
3. Claims 6, and 14-15 are canceled.
4. New claims 17-33 have been entered and approved.
5. Note it would appear that there are two typos. Claim 14 appears to be canceled and amended (note page 1 just above amended claim 1). As no amended claim 14 could be found, examiner will assume that it was the intention of the applicant to cancel the claims. A request was made to enter new claims 17-23 (page 2, just above new claim 17), however, new claims 17-33 were found in document. It will be assumed that the applicant intended the latter.
6. Previous Office actions are incorporated herein.
7. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.
8. Claims 1-5, 7-13, 16-33 are pending.

Docketing

9. Please note that the application has been redocketed to a different examiner. Please refer all future communications regarding this application to the examiner of record, using the information supplied in the final section of the office action.

Art Unit: 2766

Abstract

10. Applicant is reminded of the proper content of an abstract of the disclosure.

A patent abstract is a concise statement of the technical disclosure of the patent and should include that which is new in the art to which the invention pertains. If the patent is of a basic nature, the entire technical disclosure may be new in the art, and the abstract should be directed to the entire disclosure. If the patent is in the nature of an improvement in an old apparatus, process, product, or composition, the abstract should include the technical disclosure of the improvement. In certain patents, particularly those for compounds and compositions, wherein the process for making and/or the use thereof are not obvious, the abstract should set forth a process for making and/or use thereof. If the new technical disclosure involves modifications or alternatives, the abstract should mention by way of example the preferred modification or alternative.

The abstract should not refer to purported merits or speculative applications of the invention and should not compare the invention with the prior art.

Where applicable, the abstract should include the following:

- (1) if a machine or apparatus, its organization and operation;
- (2) if an article, its method of making;
- (3) if a chemical compound, its identity and use;
- (4) if a mixture, its ingredients;
- (5) if a process, the steps.

Extensive mechanical and design details of apparatus should not be given.

11. The applicant's Abstract appears to describe a encryption scheme with denialblilty, which is not new to the art, and yet it does not disclose anything about sequences or graphs discussed at great lengths in the specification. A new Abstract is requested which particularly describes the applicant invention and how it differs from the present state of the art.

Art Unit: 2766

Drawings

12. This application has been filed with informal drawings which are acceptable for examination purposes only. Formal drawings will be required when the application is allowed.

Specification

13. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed. Deniable Encryption as defined by Canetti, et. al. refers to a collection of encryption schemes whereby the sender can generate “fake random choices” that will make the ciphertext ‘look like’ an encryption of a different cleartext, thus keeping the real cleartext private. As is pointed out above, examples of Deniable Encryption have appeared in the art for more than 15 years, though not necessary under that name. The applicant’s invention is one example of such a scheme, but the main thrust of the invention is the use of graphical techniques to encrypt. Thus the title is not clearly indicative of the invention. Some variation on the suggested title would be more descriptive.

The following title is suggested: A Denial Cryptography Based on Graph Theory.

14. The disclosure is objected to because of the following informalities:

15. Page 9 line 21 and 22, page 41 line 16, page 70 line 5, the notation \diamond is undefined.

Art Unit: 2766

16. Page 11 line 24, the notation $0 \leq r \leq (n-1)$ is used to presumably denote $0 \leq r \leq (n-1)$, but on page 95 line 8 the notation $\sigma \geq \gamma$ which would suggest that the applicant has two different concepts in mind. If not, the notation should be uniform throughout application.
17. Page 21 line 5, the applicant uses a non standard notation (n) for the Euler function or Totient $\phi(n)$ = the cardinality of Z_n^* . This is quite confusing notation, for in line 4 applicant uses, $(b^e)^d \bmod n = b$ would seem to suggest that one should raise the number of relative primes to b^e to the d power. Suggest applicant change to standard notation to prevent confusion.
18. Page 89, line 9 space after (1).

Claim Rejections - 35 USC § 112

19. Rejection under 35 U.S.C. 112 first paragraph is withdrawn as claim 14 has been canceled.
20. Rejection under 35 U.S.C. 112 second paragraph involving claims 7, 8 and by their dependency claims 11 and 12 for lack of antecedent basis are withdrawn. Rejection of claim 15 is moot as this claim has been canceled. Claim 16 has now been amended making rejection moot.

New Claim Rejections - 35 USC § 112

21. The following is a quotation of the first paragraph of 35 U.S.C. 112:

Art Unit: 2766

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

22. Claim 1 is rejected because the symbol 1:n is nowhere defined in the specifications or in two other articles by the applicant: Leonardo/Daniel Floating-Key Cryptography and Cryptographic Possibilities Suggested by Certain Expansion-Reduction Algorithm. Not only would one of average skill in the art be required to guess the intent of the applicant, but the scope of the claim is ambiguous. As the applicant appears to be converting plaintext into a sequence of symbols that are non-repetitive, examiner will assume that this is done by placing nulls between double letters, thus "see" would become "seye". But as the nulls and text themselves are subject to frequency attack, then nulls of several letters are used such as xyz. This is interpreted as 1:3 ratio (one double letter is separated by at least three or more nulls symbols). The nulls might also be rotated xyz, yzx, zxy etc or they may rotate among a group of say three nulls, xyz, abc, uvw, etc.

Appropriate correction is required.

23. In claim 17, line 3, the term *Si symbols* are nowhere defined in the specification or the two papers mentioned above. For the purpose of prior art, the examiner will take *Si symbols* to denote a typical symbol of the sequence.

Art Unit: 2766

24. Rejection under 35 U.S.C. 102 with regards to the articles Leonardo/Daniel and Cryptographic Possibilities Suggested by Certain Expansion-Reduction Algorithm is withdraw. The applicant has claimed authorship of these articles.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

25. Claims 1-5, 7-13, 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gaines Cryptanalysis (1939).

26. In claim 1, applicant recites a method of encrypting comprising inputting a plaintext message, transforming the raw plaintext into non-repeating plaintext such that null are used to separated doubles letter in a 1:n ratio where $n > 2$, and then using the non-repeating plaintext to raw cipher by applying a reduced key and reproducing the message by applying a key to the ciphertext. By reduced key, we take the standard definition that a keys shorter than a Vernan key for a given plaintext are reduced keys.

27. Helen Gaines discloses such an encryption scheme in her book Cryptanalysis (pages 200-207). The Playfair cipher (also called the Wheatstone cipher) uses a key such as the word

Art Unit: 2766

“magnetic” and distributes the remaining letters in the order of their occurrence in rows beneath the key word. This is what is called the key array. From the key array we generate a second array used in the encryption by arranging the letters in the key array in a 5X5 square array specifying a path through the key array and using it to fill the 5X5 array. For example the path in the example below moves from M to Y then A to Z then G to R, etc.

<i>M</i>	<i>A</i>	<i>G</i>	<i>N</i>	<i>E</i>	<i>T</i>	<i>I</i>	<i>C</i>
B	D	F	H	J	K	L	O
P	Q	R	S	U	V	W	X
Y	Z						

and is used to fill the rows of the 5X5 array. We need not have used such a simple path in the filling process.

M	B	P	Y	A
D	Q	Z	G	F
R	N	H	S	E
J/I	U	T	K	V
L	W	C	O	X

Art Unit: 2766

With a different number of symbols, rectangle arrays ($27 = 3 \times 9$) may be used. Letter pairs in the plaintext may occur in one of three different ways in the 5×5 matrix: (1) The letters appear in the same row, (2) the letters appear in the same column, and (3) the letters are in different rows and column. When the letter appears in the same row, replace each of them by the letter immediately to the right (if the letter is the last column then “wrap around” to the letter in the first column of the row). When the letters appear in the same column, replace each of the by the letter immediately beneath (if the letter is in the last row then “wrap around” to the letter in the first row of the column. If the letters are neither in the same row or the same column, then replace each with the letter that is in the same row, but in the other letter’s column. (Gaines 206-207). Thus GAINES becomes FYURSH.

28. Note that the above rules do not make any provisions for double letters such as the plaintext JOHN SEE LESS MASS. Further they do not indicate how to deal with text having an odd number of letter or how to deal with spaces. Gaines addresses this on pages 4 and 201. On page 4 she introduces the general concept of a null cipher (concealment cipher), in which derives its name from the fact that one or more symbols called nulls which have no significance or used as marker, that are place in plaintext according to certain rules to conceal the true meaning of the plane text. For example nulls may be inserted between double letters to separate sentences (here X would be a marking null), to help break up the natural building blocks of the language in which the plaintext is cast (frequency attacks), placed after marking or indicator nulls (eg X...Y being makers and an, bn, cn being null) or to pad the end of a block (ie to fill out any line of

Art Unit: 2766

plane text having an odd number of symbols or for spaces, see pages 4- 5, 9, 37 55-58, and 201 of Gaines) A simple example of a null would be Y. Thus the above plaintext becomes JO HN YE YS EY EY LE SY SY MA SY SY. Generally null ciphers are re encrypted under some other cipher such as the Playfair cipher) frequency attack could determine that Y was being used as a null. To frustrate frequency attacks, we may introduce homophonic nulls which consist of several letter such as xyz, xywt, ... and further we may rotate among a set of such homophonic nulls (sometimes referred to as homophonic substitution cipher see Schneier page 10). Thus if one interpret the 1:n ratio where $n > 2$ as the homophonic nulls, for example, ratios then 1:3 would consist of sets of homophonic nulls introducing separations of 3 or more units and thus would include: xyz, tuv, swxr, vxwmz, etc. The process of modifying plaintext by the introduction of null is called by some authors, precoding, but as Gaines points out it is an encryption by itself.

29. The addition of nulls make the ciphertext a larger than the plaintext. Combinations of transposition and the Playfair substitution cipher may be accomplished by writing the plaintext in groups of N letters in two lines and then encrypting the serrated pairs with appropriate introduction of nulls (Gaines 207). Other rules for assignments can be made within the table such as replace each letter with the one two columns to the right etc. As we have taken plaintext, substituted nulls in a 1:n ratio where $n > 2$ to eliminated repetition, encrypted the non repeating plaintext with a key and a 5X5 array, finally the process may be reverse to recover the original plaintext. Thus we have meet the limitations of claim 1.

30. Claim 1 is rejected.

Art Unit: 2766

31. In claim 2 applicant recites the method of claim 1, with the further limitation that a second key is applied to the resulting cipher.

32. The limitations of claim 2 can be met by choosing a different key word (say from successive pages of a given book). Gaines discloses several variation of this with multiple substitutions and multiple alphabets. She also discloses autokeying which is the continue change of the key using the cipher text itself as a key.

33. Claim 2 is rejected.

34. In claim 3, applicant recites the method of claim 2 with the further limitation that the second key is more detailed than the first.

35. The use of say a simple shift cipher followed by a Playfair cipher is an example in which the first key is a simple shift while the second key is a word of variable length and no repeating letters. Thus the latter would be an example of a more detailed key.

36. Claim 3 is rejected.

37. In claim 4 and 5 the applicant recites the limitation that the first and second keys have starting points. And claim 8 specifies that they have different starting points.

38. By assigning the first letter of the key to the lead position of the key array we have selected a starting point. However, we could have just as well started with the third letter of the key word as our starting point, and append the first three letters to the end. Certainly we could use such a procedure for the first and second key array to gain more security. Further there is no need to have the same starting point for each key.

Art Unit: 2766

39. Claims 4, 5 and 8 are rejected.

40. Claims 6, 14, and 15 are canceled.

41. In claim 7, applicant recites a method with the limitations of claim 2, with the further limitation that the first and second keys each include a plurality of bridges, each bridge linking element an element in the non-repeating symbols. In claim 11 and 12 the bridges encompasses a two dimensional space, wherein the directions include up, down, left and right.

42. If we identify a bridge in the Playfair cipher as the path chosen through the key arrays, then certainly there are a plurality of bridges in each array and specifying a path certain line elements in the non repeating sequence of symbol, through the three rules above. Again such paths form two dimensional lattice spaces which we may specify in terms of up down left right.

43. Thus the limitations of claims 7, 11, and 12 are met. Claims 7, 11, and 12 are rejected.

44. In claim 9, applicant recite a method with the limitations of claim 1 and the further limitation that the plaintext and cipher text are different size. In claim 10, decryption of the cipher text involves a step of collapsing to obtain the plaintext.

45. Whenever nulls are used, the ciphertext is always larger than the plaintext and the decryption involves throwing out the nulls (collapsing) . Claims 9 and 10 are rejected.

46. In claim 10, applicant recites the method of claim 1, with the additional limitation

47. A Playfair cipher may be decrypted by reversing the encryption procedure. Such a reversal requires eliminating nulls thereby collapsing the results to obtain the original plaintext.

Claim 10 is rejected.

Art Unit: 2766

48. In claim 16, applicant recites a method with the limitations of claim 1, with the further limitation that the ciphertext can be matched with different potential keys.

49. Because nulls are used in a 1:n ratio, there is no one to one ratio between cipher text and keys as the homophones are rotated through a set. Claim 16 is rejected.

50. Claims 1-5, 7-13, 16, 17-³³ are rejected under 35 U.S.C. 103(a) as being unpatentable over Nakamura and Matsui (1987, 1988), and further what is well known in the art.

51. In their 1987 paper, Nakamura and Matsui develop a method of encryption in which a sequence of characters (character string) are associated with the links of a graph which uses equivalence transformation on such graphs to perform encryption (a summary of results is given in the introduction of the 1988 paper). Nakamura and Matsui 1988 deals with methods of encryption using dual graphs (page 39). As character links can be related to vectors and graphs to matrices (see section 2, pages 40-46 and in particular 2.2), one can perform many of the graph transformation by array methods with linearly dependent vectors being cast out(page 42, lines 9-10). The method provides an encryption which is comparable to a Vernan cipher (see figure 5) and such that many cipher vectors (text) are generated from the plain character vector (plaintext) by random keys (page 43 paragraph above figure 2 and figure 2). On the other hand, when a cryptanalyst tries to break the cipher text, there is a many cipher to one key for any one cipher text giving deniability. Again with equivalent graphs, there will be many graphs representing a single plaintext (which would be the analog of the nulls in Gaines Playfair ciphers). As in the case with null cipher above the ciphertext is larger than the plaintext. The key itself is a graph

Art Unit: 2766

(used to transform character links or loops in the dual space). Multiple keys can be used and each key can be identified by a starting vertex. Thus Nakamura and Matsui meet all of the limitations of claims 1-5, 7-13, 16 and hence those claims are rejected.

52. In claim 17, applicant recites an encryption method which rewrites plaintext into a sequence, creating a first encryption key, by creating a set of vertices and associating symbols with them, defining a vector space on the vertices, the vectors being associated with the symbol. Selecting a first vertex and a path from the first vertex and terminating at a second vertex. Identifying a second symbol identified to at least one vector comprising the identified path.

53. Nakamura and Matsui disclose a text string generated from a plaintext corresponding to a character graph $G_n = (V, E)$ where n is the number of vertices, V represents the vertices and E represent the links. Vectors are associated with the vertices V_i by equations (1) and (2). A path is constructed from the lines forming a loop-character vector. A second vector corresponding to this path represents the encrypted symbol (or symbol string). Claim 17 is rejected.

54. In claim 18, applicant recites a method with the limitations of claim 17 with the further limitation that to prevent consecutive symbol repetition nulls are inserted.

55. Nulls added to the symbol string may be interpreted as creating an equivalent graph in the Nakamura and Matsui discloser. This is necessary in order to get non trivial links in the graph. Claim 18 is rejected.

56. In claim 19, applicant recites a method with the limitations of claim 17, with the further limitations in which the number of vertices is at least equal to the number of symbols in the

Art Unit: 2766

plaintext and that each vertex in the set of vertices is associated with at least one terminating and at least one originating vector.

57. Nakamura and Matsui encryption would included at least as many vertices as symbols as the plaintext string, the nulls making up the difference. The collection of vertex set is defined by terminating and originating vectors as seen above. Claim 19 is rejected.

58. In claim 20, applicant recites a method with the limitations of claim 17, with the further limitation that key generation results from a set of vertices such that no two vectors originating in the same vertex are being associated with the same symbol from the second set of symbols.

59. Nakamura and Matsui use graphs to construct keys (eg. Figure 2 and section 2.3). Such graphs will not have no two vectors originating from the same vertex be associated with the same symbol otherwise the transformation is no one-to-one. Claim 20 is rejected.

60. In claim 21, applicant recites a method with the limitation of claim 17 with the further limitations that key generation where the process of creating vertices is such that a subset of contiguous vertices associated with a same symbol relates to vertices corresponding to any other symbol by vectors originating from in the subset and terminating in at least one vertex associated with a distinct symbol outside the subset.

61. Nakamura and Matsui construct key graph that are one-to-one but in such a way that equivalent graphs also have this same property. Hence even though we have a subset of equivalent graphs that are associated with the same symbol, these graphs must be distinct from other members of the set that represent other symbols. Claim 21 is rejected.

Art Unit: 2766

62. In claim 22, applicant recites a method with the limitations of claim 17, with the further limitations of informing the recipient of the sequence of symbols from the second set that correspond to the first vertex in the set of vertices (starting point for creating the sequence of symbol).

63. The starting point in the key is necessary for the recipient in order to decode the message. This is equivalent to agreeing on a key word (say in the Playfair cipher) and indicating the starting point in the key array. Claim 22 is rejected.

64. In claim 23, applicant recites a method with the limitations of claim 17, and the further limitations that from the second of two different plaintext messages, a second sequence is generated, and a second key is generated and applied to the second sequence.

65. The generation of sessions keys is well known in the art. Claim 23 rejected.

66. Claims 24-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nakamura and Matsui as applied to claims 17-23 above, and further in view of Gaines.

67. In claim 24-33, applicant recites a cryptologic methods by creating cryptanalytic obstacles the key generation method, the plaintext sequence is associated with a series of vertices in a graph and the graph in terms of a vector space in which the vertices of the sequence are marked. The keys are graphs associated with linked vertices that are linked through vectors and that the graphs are planar lattices for which each vertex has four nearest neighbors and the vector for each vertex can be described in terms of shifts up, down, left, or right on the lattice, and such that these shifts are represented by the binary codes 00, 01, 10, and 11, with the matrices being

Art Unit: 2766

expressed in binary also. That the vertices are marked using the plaintext alphabet and the vectors are marked using the ciphertext alphabet. That the cryptographic obstacles are built through expansion of plaintext.

68. Again the use of graphs to represent plaintext ciphertext and keys such that the vertex and links make me represented in terms of vector spaces and their duals were techniques disclosed by Nakamura and Matsui. The representation of these quantities in terms of binary codes has become a paradigm of the computer age. Considering a subset of graphs in which each vertex having 4 nearest neighbors, allows use to represent graphs as a planar lattice. Paths in planar lattices are defined in terms of 4 independent shift operators which may be represented in binaries. As discussed in above, Gaines also discloses null ciphers with markers in which certain nulls represent markers. As discussed above placing nulls into a plaintext string, has the results of placing one graph by an equivalent graph. Extending this to general null ciphers using markers or marking the vertices is equivalent, and so the expansion with graphs corresponds to null ciphers with markers. Claims 24-33 are rejected.

Claim Rejections - 35 USC § 102

69. Rejection of claims 1, 4, 7, 9-13 and 16 under Manual of Cryptography are maintained. See response.

Art Unit: 2766

Claim Rejections - 35 USC § 103

70. Rejection of claims 1, 2, 4, 5, and 8 under 35 U.S.C 103 in view of Schneier Applied Cryptography and what is well known in the art is maintained. See response.

Response to Arguments

71. Applicant's arguments filed 1 November 2000 have been fully considered but they are not persuasive.

72. Claims 1-5, 7-13, and 16 have been amended and claims 17-33 are new and thus arguments are moot.

73. However, with regards to the applicant's argument that Gaines does not teach converting the plaintext to a sequence of symbols, the examiner respectfully submits a plaintext in any is a linear sequence of symbols which we call an alphabet. The mapping of one sequence under a specified rule (function or relation) generates a second sequence of numbers. This can be as simple as mapping the plaintext to ASCII. As far as 1:n relation, the examiner not finding the applicant defining as to what this means with regard to his encryption scheme, took the simplest definition and concluded it might refer to a general null cipher with marker as discussed in Gaines on page 4 and 5. With regards to the Manual of Cryptography, the examiner notes that any mapping of a sequence by a specified rules (function, or relation) is a sequence $b_i = f(a_i)$. Again the 1:n relation see examiner comments above. Examiner also notes that a rejection under several pieces of art is justified if the art is used to view applicant's invention from different view points. As far as the use of nulls to break up natural building blocks of the plaintext language,

Art Unit: 2766

such as digraphs trigraphs, etc. See Gaines pages 55-58 for a discussion of frequency attacks and the use of nulls to "throw off" such attacks. The applicant argues that the use of a random key to performs encryption supersedes the need for the need for nulls and thus would not have been use by the average artisan. While this would be valid with ciphers using a Vernan encryption, using reduced keys for encryption increases the need for nulls. And as Gaines points out on page 55, military traffic often is very repetitive message format with the same dates, locations, general salutation, and closure, often filled with the same acronyms (eg. TDY, ETS, etc.), and often sent out bulk to different field commanders, makes cryptanalysis of such messages with reduced keys more susceptible to breaking. It is sometimes considered that a pseudo random generator is safe up to the time it repeats, but careful analysis of such patterns will yield. a seed long before the sequence repeats.

74. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

Art Unit: 2766

however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Conclusion

75. Any inquiry concerning this communication should be direct to James Seal at telephone number (703) 308 4562. The examiner can normally be reached on Monday through Friday from 7:30 a.m. to 5:30 p.m.

76. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gail Hayes, can be reached at (703) 305-9711.

77. Any inquiry of a general nature or relating to the status of this application or preceding should be directed to the Group receptionist, whose telephone number is (703) 305-3800. Fax number is (703) 305 0040.

James Seal



5 January 2001



**GAIL HAYES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100**